

the method further including using said data to compensate for said corruption, wherein the identification data can nonetheless be recovered from the empirical data set notwithstanding said corruption.

21. The method of claim 11 wherein there is calibration data steganographically encoded within at least one empirical data set, said calibration data having one or more known properties facilitating identification thereof during the discerning step;

the method including identifying the calibration data within the empirical data set and using data obtained thereby to aid in discerning the identification data from the empirical data set;

wherein the empirical data set has been corrupted since being encoded, said corruption including a process selected from the group consisting of: misregistration and scaling of the empirical data set;

the method further including using said data to compensate for said corruption, wherein the identification data can nonetheless be recovered from the empirical data set notwithstanding said corruption.--

REMARKS

After entry of the foregoing amendments, claims 2-21 are pending in the application. Reconsideration is requested in view of the foregoing amendments and the following remarks.

Amendment to the Specification

The March 12 Action objected to the rewritten Background discussion, contending that it introduced new matter.

Applicant believes that rewriting - of the type proposed - finds precedent in other cases. One example is U.S. patent 5,694,603, where the applicant entirely rewrote the Background description to employ terminology and details not literally included in the application as originally filed. (The '603 patent was pending over fifteen years, and was thrice reviewed by the Board of Appeals.)

Although the earlier rewriting is believed proper, applicant has deleted the earlier-added text, and substituted different text above. The bulk of the text simply paraphrases the pending claims.

New Claims

New dependent claims 20 and 21 introduce the feature of calibration data included in at least one of the empirical data sets, permitting recovery of the identification data even if the empirical data has been corrupted by re-scaling or re-registration of the video/audio/imagery represented thereby. These claim limitations are modeled after claim 26 in applicant's patent 5,636,292. Support for these limitations is found, e.g., in the section entitled Rings to Knots (pp. 50 et seq) of the present specification.

Response to Factual Arguments re Powell (MPEP § 707.07(f))

The March 12 rejections based on Powell repeat the same rejection language from the September 24 Action, updated simply to conform to the issued Powell U.S. patent, rather than the earlier-cited published EP Powell application.¹

The Office failed to respond to applicant's detailed arguments, filed December 15, particularly rebutting each of the factual underpinnings on which such rejections were earlier based.

MPEP § 707.07(f) requires the Office to take note of applicant's arguments, and answer same.

If the rejections based on Powell are renewed and made final, the Examiner is asked to comply with this MPEP section so as to better focus the issues for appeal. For the Examiner's convenience, applicant's earlier remarks distinguishing Powell are reproduced in italics:

Powell discloses a method and system for creating digital image signatures. Applicant respectfully submits that Powell does not teach the claimed combinations.

Powell does not appear to disclose the automatic downloading of data, including empirical data sets, from a plurality of computer sites over the internet. The internet is not

¹ The present assignee is now the record owner of the Powell patent, and is prosecuting a continuation thereof.

referenced in Powell. Moreover, nothing indicates any automatic downloading, or any downloading. (Automatic is in contrast with manually specifying each data set to be downloaded.)

Powell page 2, lines 8-13 is understood to teach simply that images can be distributed in print and electronic form. Page 3, lines 21-34 is understood to review how a print image can be converted to digital form with a scanner. The scanner output can be stored on a diskette for displaying later at a remote site.

Nor does Powell appear to disclose automatic screening of each of plural empirical data sets obtained by the downloading operation, to identify the potential presence of identification data steganographically embedded therein.

Page 5, lines 15-50, is understood to disclose how a suspect image can be normalized preparatory to performing a watermark analysis. Such an operation does not "identify the potential presence of identification data."

Powell teaches the discerning of identification data from a suspect image. However, this operation is not performed on plural images. Nor is it performed on images that have first passed a screening operation. The cited excerpt at page 5, line 51 through page 6, line 14, is not understood to teach any of these latter elements.

Finally, Powell is not understood to teach generating a report identifying steganographically encoded empirical data sets identified as above, and the site from which each was downloaded.

Page 2, lines 8-23, describes the Background of the Powell work, and reviews the need for a marking technology that allows the proprietor of an image to confirm that a suspect image is derived from his work – a marking that can withstand various modifications. Page 5, lines 12-18, briefly reviews the steps of normalizing a suspect image, and analyzing same to extract any embedded data.

In view of these and other failings of Powell, claim 2 is not anticipated by such art and should be in condition for allowance.

Claims 3-10 all depend from claim 2 and should similarly be allowable. Each is also patentable independent from claim 2.

For example, claim 3 defines a method employing a master code signal that is used in discerning the steganographically encoded identification data from the screened empirical data sets. No master code signal is disclosed in Powell.

The excerpt at page 5, line 36, through page 6, line 14, is understood to teach how to normalize the brightness, contrast and/or color of the suspect image to conform to that of the original image, by reference to the brightness/contrast/color of selected pixels in the original image. Once normalized, the suspect image is subtracted from the original image to identify changes to the Powell's "signature points." (Or the suspect image can be compared with the signed image to determine whether the changes to the signature points match.)

Claim 3 also indicates that one master code signal is used to discern steganographically encoded data from "a plurality" of the screened data sets. Thus, if the locations of Powell's signature points were somehow regarded as a master code signal, those locations are unique to that image, and are not uniformly applied to all of a plurality of images downloaded from the internet.

Claim 4 specifies that the master code signal has the appearance of unpatterned snow if represented in the pixel domain. Figs. 2, 3 and 5 are not understood to disclose this feature. Figs. 2 and 5, for example, show a sample digital image (page 2, line 54 - page 3, line 2), not a master code signal. Moreover, the image is clearly patterned, showing a head in profile.

Similarly, Fig. 3 shows pixel values corresponding to an image excerpt, not an unpatterned master code signal.

Claim 5 specifies that the discerning of the identification data is accomplished without previous knowledge of the audio, image, or video information represented thereby.

Powell teaches just the opposite. In order for Powell to decode a suspect image, he must have either (1) the original (unsigned) image, or (2) the originally signed image. This is evident from the excerpt cited in the Action.

Claim 6 defines a method that includes identifying proprietors of empirical data sets by reference to identification data discerned therefrom, and reporting to said proprietors the sites from which their data sets were downloaded.

Powell teaches that a binary number between 16 and 32 bits in length is encoded into an image (page 3, lines 46-47). However, this number does not allow the proprietor of the image to be identified. Rather, it allows the proprietor of the work to confirm that the image is his own.

Powell contemplates that the person analyzing the suspect image is its proprietor -- analysis requires access to the original (unsigned) image, or the originally-signed image. A person who did not already know the identity of the proprietor wouldn't know where to look in the image for signature points. Thus, Powell's binary number simply serves as an arbitrary hallmark whose presence in a suspect image cannot be simply disregarded as happenstance.

Still further, nothing in Powell teaches "reporting to said proprietors the sites from which their empirical data sets were downloaded."

Claim 7 defines a method that includes encoding information in addition to data identifying the proprietor. Since Powell's binary number is an arbitrary tag that allows a suspect and an original image to be correlated, no additional data is represented thereby.

Claim 8 defines a method in which the identification data is a serial number index into a registry database containing names and contact information for proprietors identified by the identification data.

As noted, Powell's binary number is an arbitrary marking. However, apart from this distinction, Powell also does not teach use of his encoded number as an index into a registry database containing names and contact information.

Claim 9 defines a method in which the discerning operation includes performing a plurality of statistical analyses on the pixel-form image. Powell employs a deterministic detection method in which the outcome is based on the values of a few specific pixels. He does not teach an arrangement in which the embedded information is discerned as the result of plural statistical analyses, each of which relies on statistical characteristics of the image.

Claim 10 further defines the statistical analysis as including analyzing a collection of spaced apart pixels to decode a single, first bit of the identification data, said analysis encompassing not just the spaced apart pixels, but also pixels adjacent thereto, where the adjacent pixels are not encoded with that first bit.

Powell does not teach such an arrangement.

Powell may be interpreted as examining a collection of spaced apart pixels to decode a first bit, because he teaches that each bit may be redundantly encoded at several different locations.

However, that analysis by Powell does not meet the further limitation of claim 10, namely that the analysis to decode the first bit encompasses "not just the spaced apart pixels, but also pixels adjacent thereto, said adjacent pixels not being encoded with said first bit." Powell, in contrast, examines the values just at the "signature point" pixels; the tapering of

pixel values therearound is to reduce the human visibility of artifacts of the encoding. Moreover, the pixels adjacent Powell's signature points are encoded in accordance with the same bit with which the signature bit is encoded (being changed in proportionately tapered fashion) – again contrary to the claim's requirement.

Claim 11 defines a method for surveying distribution of proprietary empirical data sets on computer sites accessible via the internet. Again, Powell does not mention the internet, nor any method or surveying distribution of proprietary material on computer sites accessible via the internet.

Claim 11 further requires provision of a master code signal useful for detecting steganographic coding within empirical data sets. The claimed master code signal is employed with each of "a plurality" of empirical data sets.

As discussed above in connection with claim 3, Powell has no disclosure of such a master code signal useful for detecting steganographic coding within plural empirical data sets.

Claim 11 further requires automatic downloading of data, including empirical data sets, from a plurality of computer sites over the internet. Again, as discussed above in connection with claim 2, Powell does not teach such an arrangement.

Claim 11 further requires – for each of plural empirical data sets obtained by said downloading operation – discerning certain identification data, if any, steganographically encoded therein, said discerning employing said master code signal as a decoding key.

Again, as discussed previously, Powell makes no use of a single master code signal as a decoding key for plural sets of empirical data.

Claim 11 further requires generating a report identifying steganographically encoded empirical data sets identified by the foregoing steps, and the site from which each was downloaded. Again, as discussed above, Powell does not generate a report. He does not download data. He does not detail which site contained which empirical data.

In view of these and other failings of Powell, claim 11 is not anticipated by such art and should be in condition for allowance.

Claims 12-20 are allowable for the reasons discussed above in connection with claims 2-10.

Answering Asserted Advantages

In the December 15 Amendment, applicant detailed advantages provided by the claimed combinations that are not provided by the art.

The MPEP advises that such advantages should be addressed by the Examiner in responding to Amendments. Otherwise, such advantages are deemed admitted for purposes of appeal. (MPEP § 707.07(f)).

As noted in the December 15 Amendment, the presently-claimed methods allow image proprietors and the like to locate web sites to which their images, etc. have been posted. A report is periodically provided to content owners detailing where their works were found. (A sample

report, entitled *MarcSpider Report for August, 1997*, is attached.) The owners can then take whatever action is appropriate in the circumstances.

Applicant particularly noted the experience of Playboy, whose images are commonly pirated over the internet. Playboy employs the MarcSpider service of the present assignee (which practices the claimed methods) to churn through myriad images posted on the world wide web, and report back to Playboy regarding sites where Playboy imagery is found.

None of the prior art teaches or suggests such advantages.

Long Felt Need

The need served by the claimed invention (e.g. the need to find where proprietary image data and the like have been distributed) is as old as the internet² -- the innovation which first made possible the unrestricted distribution of digital files between computers. The need grew acute with the introduction of the graphical world wide web, where imagery proliferates.

This need has been widely recognized and acknowledged in press coverage of applicant's MarcSpider product (which, as noted, practices the claimed inventions).

Attached, for example, is an excerpt from MacWorld magazine entitled "Safeguard Your Art." The article notes:

No matter how much proof you have that you own an image, it won't do you any good if you don't know who's taken it. Since visitors to your Web site don't leave foot- or fingerprints, you're faced with a lot of Web surfing and magazine reading if you want to try to find images that may have strayed from their rightful locations.

Fortunately, Digimarc has addressed part of this problem as well. The recently released MarcSpider is a Web-based agent that prowls the Web searching for PictureMarc-encoded images...³

This need remained unmet until applicant's invention. This long felt but unmet need is additional evidence of the invention's patentability.

More generally, content providers were long reluctant to publish their imagery/audio/video on the web (i.e. in digital form) -- fearing that by so doing, they would lose

² The Office cites Shear's '594 patent, *filed in 1986*, as teaching the downloading of data from plural computer sites over the internet.

control of their content due to uncontrollable copying. The present invention overcame this obstacle.

This impediment to web publication has long been understood in the industry, and is noted, e.g., in the attached excerpt from DEC's journal "The Rapidly Changing Face of Computing." In discussing Playboy's adoption of the MarcSpider service, the article notes:

There may be some unhappy people out there as Playboy's lawyers follow up MarcSpider's leads, but this is a good omen for The Net. The sooner that publishers of all media feel comfortable that they can safely distribute their works in digital form, the sooner we will have an even greater field of information to harvest at our fingertips.

The problem was well stated six years ago in a 1992 program by Northwestern University entitled *The Annenberg Washington Program in Communications*, which noted, "[W]hen creative works are on a computer network, the creator gives up control so there is reluctance to make materials available on-line." (Page 2, attached.)

The present invention solves this long felt need.

Copying By Others

Imitation is the sincerest form of flattery, and several companies in the industry have paid tribute to the inventiveness of applicant's work by copying same (or advertising their intention to do so). This is further evidence of the invention's patentability.

Attached, as one example, is a Frequently Asked Questions document published by Signum Technologies, a UK company which offers its SureSign image watermarking products and services in competition with the present assignee. That document notes (page 2):

3. Can SureSign be used to monitor the distribution of copyright material?

SureSign technology makes it possible to examine and thus determine the source of fingerprinted images that have been posted on web sites, or distributed on-line or by CD-ROMs. The format of the fingerprint is well suited to computerised monitoring using search engines and spiders and, thus in the future, will allow content providers to automatically audit the use of their material. The resultant data could be used to facilitate automated billing. Signum Technologies expect to offer a web search service in the near future.

Attached, as a second example, is a March 3, 1998, press released issued by another competitor (Working Knowledge) which touts its competing technology as follows (page 2):

First, this new technology uses a repeat and embedded fingerprinting system which can survive 20x jpeg compression as well as software alterations and hardcopy printing.

Second, two tracking devices called Web Patrol and Aurora Spider (with its search engine J. Edgar) track the transmission through all its points and can locate any unauthorized access and use.

As a third example – this one in the audio field – attached is a White Paper published by Intersect, Inc. After discussing the digital watermarking of audio, the paper notes how such watermarks are used to track distribution of audio on the Internet (page 4):

Intersect searches, tracks, and monitors the Internet. Using Audio Video Scan (AVS) technology, Intersect searches up to eleven million Web pages per day, with the ability to scan the entire Internet – currently over 54 million Web pages – in just two weeks, faster than any other spider technology.

If the claimed combinations were obvious, such product offerings would have been made years ago. Instead, it was not until the present assignee publicized its service that these competitors jumped on the bandwagon. This is still further evidence of the invention's non-obviousness.

Commercial Success, Evidenced by Playboy's Adoption of Claimed Technology

As still further evidence of the claimed technology's non-obviousness, the Examiner is requested to consider the earlier-submitted articles discussing Playboy's adoption of the claimed technology. Playboy is a leading provider of imagery, and has the dubious distinction of being the most pirated image source on the web. As is evident from those articles, the advantages provided by applicant's claimed technology – advantages not otherwise available – were key in Playboy's decision to adopt this technology. Such adoption by this market leader is yet further evidence of the invention's non-obviousness.

Request For Interview

The Examiner is formally requested to contact the undersigned attorney prior to issuance of the next Office Action in order to arrange a telephonic interview. It is believed that a brief

discussion of the merits of the present application will expedite prosecution or better focus the issues for appeal. Applicant submits the foregoing formal Amendment so that the Examiner may fully evaluate Applicant's position, thereby enabling the interview to be more focused.

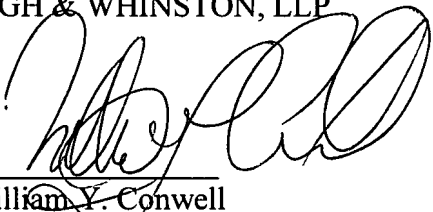
This request is being submitted under MPEP § 713.01, which indicates that an interview may be arranged in advance by a written request. Moreover, the MPEP indicates that the interview should be granted unless the Examiner has a compelling reason to refuse such an interview.

Favorable consideration is requested.

Respectfully submitted,

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
cc: Geoff Rhoads

By 
William Y. Conwell
Registration No. 31,943